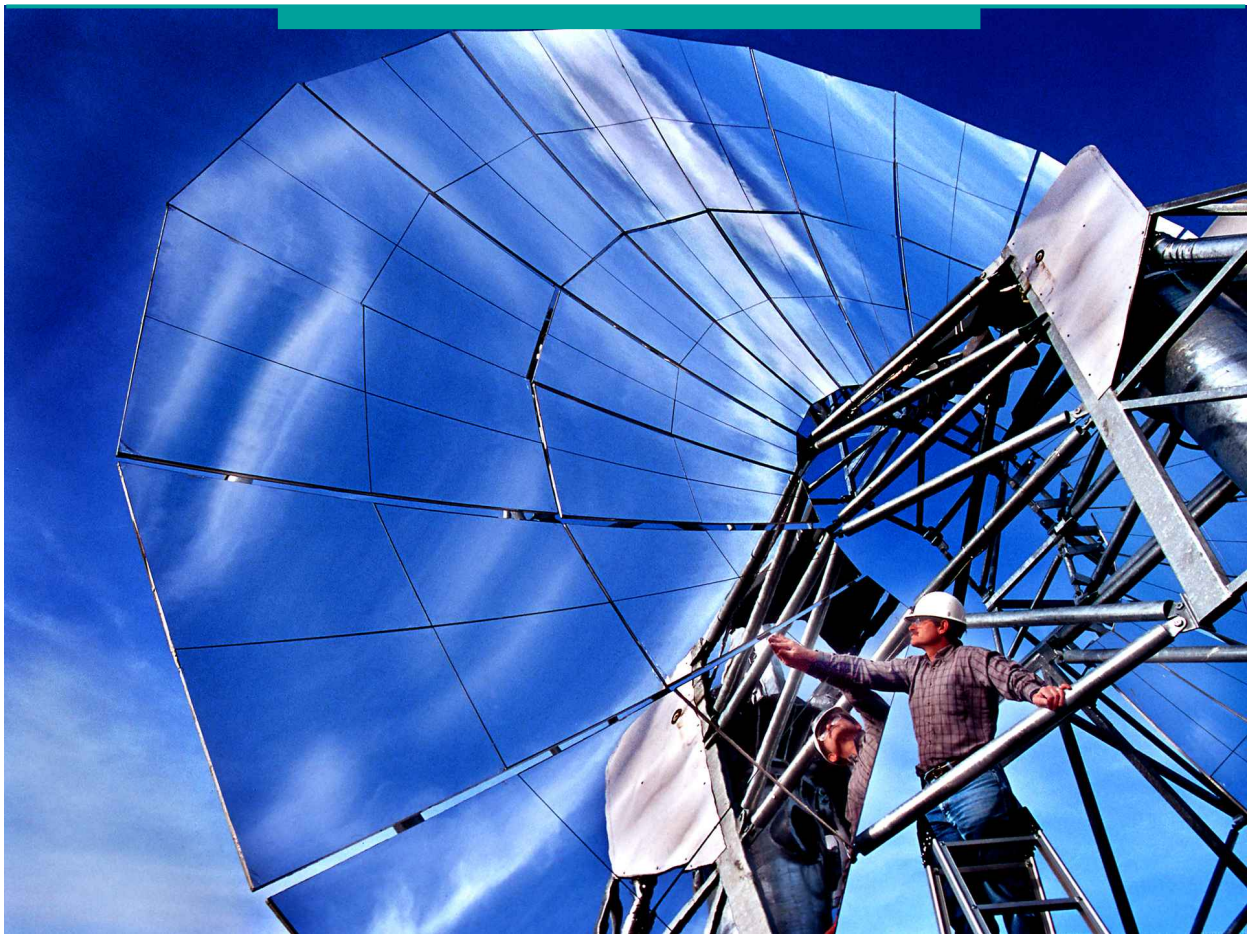
Dish/Stirling

Provides Test for Secure Control System

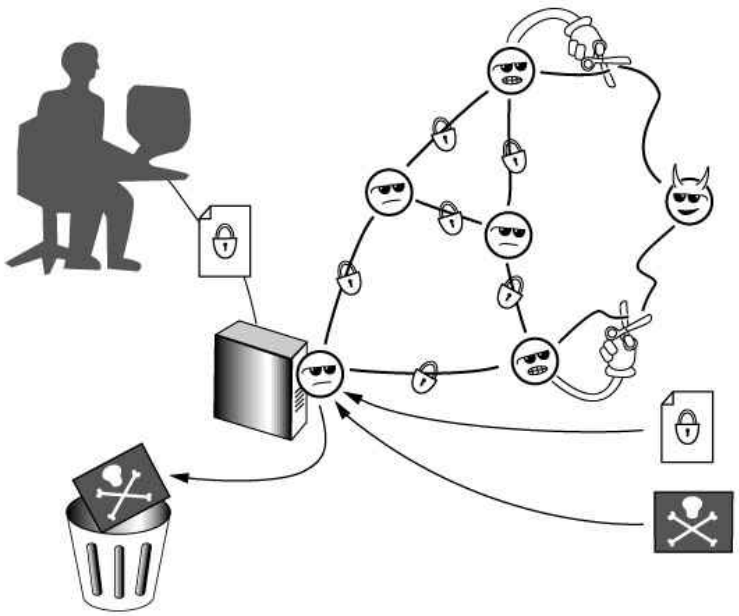


Program manager Richard Diver inspects the Dish/Stirling remote power system.

The 500-square-foot mirrored dish at Sandia's National Solar Thermal Test Facility represents a milestone in harnessed solar power. A mechanical heliotrope, the dish tracks the sun, focusing its heat onto a receiver, which collects and transfers it to a Stirling heat engine. The engine is a sealed system filled with gas, and as the gas heats and cools, its pressure rises and falls. The change in pressure is controlled to make the pistons inside the engine move, producing mechanical power. The mechanical power in turn drives a generator and makes electricity.

Key to the success of the Dish/Stirling is its supervisory control and data acquisition capability, which allows it to be controlled and monitored from a distance.

Key to the success of the Dish/Stirling system is its supervisory control and data acquisition (SCADA) capability, which allows it to be controlled and monitored from a distance. A research team remotely controls the dish's angles, motor speed, and other operational details. The



Agents in a collective communicate over secure links on the internet or an intranet. Malicious agents (with horns) are detected and cut off from the collective. Properly authenticated data are allowed into the collective, but bad information is rejected.

Dish/Stirling's 10 kW generator and its overall architecture reflect on a small scale the direction in which the renewable energies industry is headed. The lessons learned from Dish/Stirling, particularly in developing a secure SCADA system, eventually will be applied industrywide, said Rolf Carlson, a principal investigator for high surety SCADA research at Sandia.

"Sandia's reliability and security R&D focuses on real-time responses to unforeseen events. Our goal is to develop the capability to keep the power on, even under adverse circumstances," Carlson said.

The utility industry has not always faced security concerns. Prior to deregulation and the advent of smaller utility systems, utilities had their own proprietary systems, each one offering a modicum of security. Today, the migration toward open systems and networking has led to the creation of industry standards and made shared protocols a necessity.

"Faced with deregulation and the need to move information quickly and seamlessly across company environments, the utility companies are having to determine what information to share and how to protect it," explained Juan Torres, a principal investigator on distributed energy resources projects. "The systems now being brought online by the utilities must incorporate security features. Sandia's work in security and sensor technologies is part of that evolution towards secure systems—we are weaving security deeper and deeper into the distributed energy control systems environment."

Sandia's SCADA technology draws upon its vast experience in nuclear systems security and safeguards. The goal is to develop economical, compact solutions. Software fills the bill on both counts.

Sandia is incorporating authentication and cryptographic protocols, centralized or decentralized control, firewalls, and other features into its SCADA systems. Much of this work stems from its partnerships with companies like Quetana Systems (formerly Communication Systems Technology, Inc.), an Albuquerque-based producer of remote control and monitoring products including LongArm® Network/Communication software and SecureCloud software. Other Sandia partners include MCI Worldcom, Cisco, and Raytheon.

Sandia's SCADA technology draws upon its vast experience in nuclear systems security and safeguards. The goal is to develop economical, compact solutions. Software fills the bill on both counts.

Once the security enhancements are in place, Sandia's "Red Team" conducts a systems vulnerability analysis by trying to break through the security system. The team analyzes both design methodology and the efficacy of equipment. "What the energy industry needs is a unified control architecture for critical infrastructures," said Torres. "A number of open protocols exist but they were not being put together in a secure way."

Sandia is taking a proactive role in facilitating the design of total system security for the next generation of SCADA by partnering for technology development, by helping users to implement their systems, by participating on standards committees, and by cooperating with vendors who are generating the security markets.

TECHNICAL CONTACTS:
Rich Diver
505-844-0195
rbdiver@sandia.gov

Juan Torres
505-844-0809
jjtorre@sandia.gov